Partnership combines INL's Constrained Cyber Communication Device with *Binary Armor*® to protect critical infrastructure

By Cory Hatch for INL communications

While most electric utilities rely on perimeter security systems such as firewalls or segmented networks to prevent a cyberattack, these security measures can't protect vital equipment once that perimeter is breached.

Idaho National Laboratory researchers recently developed a technology that provides an extra layer of protection by repelling cyberattacks at the location of equipment itself.

The Constrained Cyber Communication Device (C3D) works by limiting the exposure of critical infrastructure—protective relays—to outside communications while maintaining operations.

Protective relays are leading targets of cyberattacks because they play a key role in the grid by safeguarding equipment and ensuring stability of the grid. C3D gives utilities time to defend against a cyberattack by a limiting protective relay's exposure.

Caption: INL's Jake Gentle, Steve Bukowski, and Dylan Reen stand with the patent-pending Constrained Communications Cyber Device (C3D) in their field deployable test setup.

In March, INL researchers entered into a partnership with Sierra Nevada Corporation (SNC) to combine C3D with Sierra's *Binary Armor*® SCADA network cybersecurity tool.

Binary Armor protects control systems, infrastructure and personnel from cyberthreats and human error by allowing only preapproved, safe messages to reach operational technology.

Together, the tools provide a layered approach to protecting our nation's critical infrastructure systems.

"Combining INL technology with Sierra Nevada's Binary Armor is a perfect example of government and industry working together to solve a critical national challenge," said Jake Gentle, INL program manager and C3D developer. "Grid technology is advancing and becoming more secure every day. But we still need to protect millions of devices that are currently in service."

The two systems, working in tandem, will add resiliency to the grid and protect infrastructure automatically, while also alerting system administrators to the cyberattack attempts and allowing the systems to continue running uninterrupted even if there is a breach.

"As the cyberthreats to our critical infrastructure and operational technology continue to evolve and grow more dangerous, Binary Armor has been on the front lines to keep our communities safe," said Peter Fischer, SNC's director of cybersecurity programs. "Now, enhanced by INL's industry-leading expertise and innovative technology, Binary Armor + C3D will help us stay one step ahead of evolving threats to keep the lights on, the water flowing and our nation moving forward securely."

Idaho researchers demonstrated C3D's effectiveness in stopping cyberattacks in tests at a 36-foot mobile substation connected to Idaho National Laboratory's Critical Infrastructure Test Range Complex, a full-scale electric power grid test bed.

Caption: To demonstrate the ability of the C3D to block a cyberattack on the power grid, researchers constructed a 36-foot long mobile substation and connected it to INL's full-scale Power Grid Test Bed.

During the demonstration, researchers tested the C3D against a series of remote access attempts indicative of a cyberattack. The device alerted operators to the abnormal commands—including a sudden power spike demand—and blocked them automatically, preventing the attacks from accessing and damaging critical power grid components.

The C3D testing was successful, effectively disabling access to the relay while maintaining its monitoring and control capabilities.

INL also demonstrated C3D at an event for electric utility professionals hosted by the Western Area Power Administration. The demonstration allowed C3D to be setup and configured to protect a relay within the Electric Power Training Center, a hands-on training facility used by many of the nation's operations and dispatch professionals.

Caption: INL researchers demonstrated the Constrained Cyber Communication Device during a live exercise for representatives of the Western Area Power Administration.

Further, C3D is low cost and low maintenance—it provides utilities with a cybersecurity solution that won't cost millions of dollars in training, service or upgrades.

Binary Armor has been tested and validated by both U.S. Department of Defense and industry labs with continuous operation since 2014 on utility SCADA and control systems.

Click here to watch a video on this technology.

For more information, visit: https://inl.gov/critical-infrastructure-protection/prpc/